(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平8－249286

(43)公開日　平成８年(1996)９月27日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	15/00	３３０	9364－5L	Ｇ０６Ｆ	15/00	３３０Ｚ
Ｇ０７Ｂ	1/00			Ｇ０７Ｂ	1/00	Ａ
Ｇ０９Ｃ	1/00		7259－5Ｊ	Ｇ０９Ｃ	1/00	
Ｈ０４Ｌ	9/06			Ｈ０４Ｌ	9/02	Ｚ
	9/14					

審査請求　未請求　請求項の数17　ＯＬ　（全 15 頁）

(21)出願番号　特願平7－54069

(22)出願日　平成７年(1995)３月14日

(71)出願人　000002945
オムロン株式会社
京都府京都市右京区花園土堂町10番地

(72)発明者　出水　法俊
京都府京都市右京区花園土堂町10番地　オムロン株式会社内

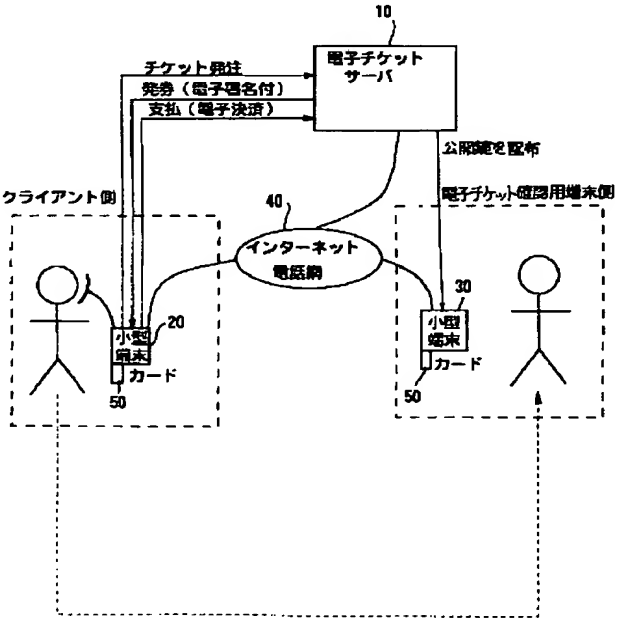
(74)代理人　弁理士　和田　成則

(54)【発明の名称】　電子データ送受信システム

(57)【要約】

【目的】　送信された電子データの不正利用を防止するとともに、データ送信の秘密の保持性に優れた電子データ送受信システムを提供する。

【構成】　サーバ端末（１０）は、クライアント端末（２０）からの送信要求に対応して暗号化した通し番号を付与した電子データをクライアント端末（２０）に送信するとともに、送信した電子データを記憶し、また、クライアント端末（２０）は、サーバ端末（１０）から送信された電子データを受信してカード５０に書き込むことにより電子データの受信を行い、また、チェッカ端末（３０）は、カード（５０）に書き込まれた電子データとサーバ端末（１０）に記憶した電子データとを照合することにより電子データの確認を行う。



1

【特許請求の範囲】

【請求項１】　電子データを送信するサーバと該サーバから送信された電子データを受信するクライアントと該クライアントで受信した電子データの確認を行う電子データ確認端末とを具備する電子データ送受信システムにおいて、

上記サーバは、

上記クライアントからの送信要求に対応して暗号化した通し番号を付与した電子データを上記クライアントに送信する電子データ送信手段と、

上記電子データ送信手段で送信した電子データを記憶する電子データ記憶手段とを具備し、

上記クライアントは、

上記電子データ送信手段により上記サーバから送信された電子データを受信することにより上記電子データの受信を行う電子データ受信手段を具備し、

上記電子データ確認端末は、

上記電子データ受信手段で受信した電子データと上記電子データ記憶手段に記憶した電子データとを照合することにより上記電子データの確認を行う電子データ確認手段を具備することを特徴とする電子データ送受信システム。

【請求項２】　上記電子データ送信手段は、

上記クライアントからの送信要求に対応して電子データを生成する電子データ生成手段と、

上記電子データ生成手段で生成された電子データに暗号化した通し番号を付与する通し番号付与手段と、

上記通し番号付与手段で暗号化した通し番号が付与された電子データを上記クライアントに送信する送信手段と、

を具備することを特徴とする請求項１記載の電子データ送受信システム。

【請求項３】　上記クライアントは、

上記電子データを書き込み可能なカードを有し、

上記電子データ送信手段により上記サーバから送信された電子データを受信して上記カードに書き込むことにより上記電子データを受信することを特徴とする請求項１記載の電子データ送受信システム。

【請求項４】　上記電子データ確認端末は、

上記クライアントで受信した電子データの電子データに付与された暗号化した通し番号を解読することにより上記電子データの確認を行うことを特徴とする請求項１記載の電子データ送受信システム。

【請求項５】　上記電子データ送信手段は、

上記クライアントからの送信要求に対応して電子データを生成する電子データ生成手段と、

上記電子データ生成手段で生成された電子データに暗号化した通し番号を付与する通し番号付与手段と、

上記通し番号付与手段で暗号化した通し番号が付与された電子データの全体を暗号化する暗号化手段と、

2

上記暗号化手段で暗号化した電子データを上記クライアントに送信する送信手段と、

を具備することを特徴とする請求項１記載の電子データ送受信システム。

【請求項６】　上記クライアントは、

上記暗号化手段で暗号化された電子データを解読する解読手段を具備することを特徴とする請求項５記載の電子データ送受信システム。

【請求項７】　電子データを送信するサーバと該サーバから送信された電子データを受信するクライアントと該クライアントで受信した電子データの確認を行う電子データ確認端末とを具備する電子データ送受信システムにおいて、

上記クライアントは、

上記サーバに対して上記クライアント側で作成した暗号キーワードを含む電子データの送信を要求する送信要求手段を具備し、

上記サーバは、

上記クライアントからの送信要求に対応して上記暗号キーワードを含む電子データを上記クライアントに送信する電子データ送信手段と、

上記電子データ送信手段で送信した電子データを記憶する電子データ記憶手段とを具備し、

上記クライアントは、

上記電子データ送信手段により上記サーバから送信された電子データを受信する電子データ受信手段を具備し、

上記電子データ確認端末は、

上記電子データ受信手段で受信した電子データと上記電子データ記憶手段に記憶した電子データとを照合することにより上記電子データの確認を行う電子データ確認手段を具備することを特徴とする電子データ送受信システム。

【請求項８】　上記送信要求手段は、

上記クライアント側で作成した暗号キーワードを含む電子データの送信要求の全体を暗号化して上記サーバに対して送信することを特徴とする請求項７記載の電子データ送受信システム。

【請求項９】　上記電子データ送信手段は、

上記暗号キーワードを含む電子データの全体を暗号化して上記サーバに対して送信することを特徴とする請求項７記載の電子データ送受信システム。

【請求項１０】　上記クライアントは、

上記暗号化手段で暗号化された電子データを解読する解読手段を具備することを特徴とする請求項９記載の電子データ送受信システム。

【請求項１１】　電子データを送信するサーバと該サーバと回線を介して接続され該サーバから送信された電子データを受信するクライアントとを具備する電子データ送受信システムにおいて、

上記クライアントは、

上記電子データの送信要求を生成する送信要求生成手段と、
上記送信要求生成手段で発生された送信要求を上記クライアントの秘密鍵を用いて暗号化する第１の暗号化手段と、
上記第１の暗号化手段に暗号化された送信要求を上記サーバの公開鍵を用いて暗号化する第２の暗号化手段と、
上記第２の暗号化手段で暗号化された送信要求を上記サーバに送信する送信要求手段と、
を具備することを特徴とする電子データ送受信システム。

【請求項１２】　上記サーバは、
上記送信要求手段により送信された送信要求を受信する送信要求受信手段と、
上記送信要求受信手段で受信した送信要求を上記サーバの秘密鍵を用いて復号化する第１の復号化手段と、
上記第１の復号化手段で復号化された送信要求を上記クライアントの公開鍵を用いて復号化することにより上記送信要求の適否の照合を行う第１の照合手段と、
上記第１の照合手段により上記送信要求が適正であると判定された場合は、上記送信要求に対応する電子データを生成する電子データ生成手段と、
上記電子データ生成手段で生成された電子データに暗号化した通し番号を付与する通し番号付与手段と、
上記通し番号付与手段で暗号化した通し番号が付与された電子データを上記サーバの秘密鍵を用いて暗号化する第３の暗号化手段と、
上記第３の暗号化手段で暗号化された電子データを上記クライアントの公開鍵を用いて暗号化する第４の暗号化手段と、
上記第４の暗号化手段で暗号化された電子データを上記サーバに送信する電子データ送信手段と、
を具備することを特徴とする請求項１１記載の電子データ送受信システム。

【請求項１３】　上記クライアントは、
上記電子データ送信手段から送信された電子データを受信する電子データ受信手段と、
上記電子データ受信手段で受信した電子データを上記クライアントの秘密鍵を用いて復号化する第２の復号化手段と、
上記第２の復号化手段で復号化された電子データを上記サーバの公開鍵をを用いて復号化することにより上記電子データの適否の照合を行う第２の照合手段と、
上記第２の照合手段で上記電子データが適正であると判定された場合は、上記電子データを記録する記録手段と、
を具備することを特徴とする請求項１１記載の電子データ送受信システム。

【請求項１４】　電子データを送信するサーバと該サーバと回線を介して接続され該サーバから送信された電子データを受信するクライアントとを具備する電子データ送信システムにおいて、
上記クライアントは、
上記電子データの送信要求を生成する送信要求生成手段と、
上記送信要求生成手段で発生された送信要求に乱数を付与する乱数付与手段と、
上記乱数付与手段で乱数が付与された送信要求を上記クライアントの秘密鍵を用いて暗号化する第１の暗号化手段と、
上記第１の暗号化手段で暗号化された送信要求を上記サーバの公開鍵を用いて暗号化する第２の暗号化手段と、
上記第２の暗号化手段で暗号化された送信要求を上記サーバに送信する送信要求手段と、
を具備することを特徴とする電子データ送受信システム。

【請求項１５】　上記サーバは、
上記送信要求手段により送信された送信要求を受信する送信要求受信手段と、
上記送信要求受信手段で受信した送信要求を上記サーバの秘密鍵を用いて復号化する第１の復号化手段と、
上記第１の復号化手段で復号化された送信要求を上記クライアントの公開鍵を用いて復号化することにより上記送信要求の適否の照合を行う第１の照合手段と、
上記第１の照合手段により上記送信要求が適正であると判定された場合は、上記送信要求に対応する電子データを生成する電子データ生成手段と、
上記電子データ生成手段で生成された電子データを上記サーバの秘密鍵を用いて暗号化する第３の暗号化手段と、
上記第３の暗号化手段で暗号化された電子データを上記クライアントの公開鍵を用いて暗号化する第４の暗号化手段と、
上記第４の暗号化手段で暗号化された電子データを上記サーバに送信する電子データ送信手段と、
を具備することを特徴とする請求項１４記載の電子データ送受信システム。

【請求項１６】　上記クライアントは、
上記電子データ送信手段から送信された電子データを受信する電子データ受信手段と、
上記電子データ受信手段で受信した電子データを上記クライアントの秘密鍵を用いて復号化する第２の復号化手段と、
上記第２の復号化手段で復号化された電子データを上記サーバの公開鍵をを用いて復号化することにより上記電子データの適否の照合を行う第２の照合手段と、
上記第２の照合手段で上記電子データが適正であると判定された場合は、上記電子データを記録する記録手段と、
を具備することを特徴とする請求項１４記載の電子デー

タ送受信システム。

【請求項１７】　電子データを送信するサーバと該サーバから送信された電子データを受信するクライアントと該クライアントで受信した電子データの確認を行う電子データ確認端末とを具備する電子データ送受信システムにおいて、

上記クライアントは、

上記サーバから送信された電子データに対応する上記サーバの秘密鍵を用いて暗号化された電子データを記憶する記憶手段と、

上記記憶手段に記憶された上記電子データを取り出す取出手段と、

上記取出手段により取出された電子データを上記電子データ確認端末の公開鍵を用いて暗号化する暗号化手段と、

上記暗号化手段で暗号化されたデータを上記電子データ確認端末に送信する送信手段と、

を具備し、

上記電子データ確認端末は、

上記送信手段により送信された電子データを受信する受信手段と、

上記受信手段で受信した電子データを上記電子データ確認端末の秘密鍵を用いて復号化する復号化手段と、

上記復号化手段で復号化した電子データの適否を確認する確認手段と、

を具備することを特徴とする電子データ送受信システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】この発明は電子データ送受信システムに関し、特に送信された電子データの不正利用を防止するように改良した電子データ送受信システムに関する。

【０００２】

【従来の技術】最近、Ｓ－ＲＡＭやＥＥＰ－ＲＯＭ等の半導体メモリを内蔵したＩＣカードを用いることにより、ホテルの利用チケット、電車、飛行機、船のチケット、映画館、コンサートのチケットなどをインターネット電話網を介して電子的に発券する電子チケット発券システムが考えられている。この電子チケット発券システムとしては、従来、特開平６－２３６４６４号公報に開示されたものが知られている。

【０００３】ところで、この種の電子チケット発券システムは、一般には、電子チケットを発券するサーバと該サーバから発券された電子チケットを受券するクライアントと該クライアントで受券した電子チケットの確認を行う電子チケット確認端末とを具備して構成されるが、ここで、サーバから発券されるチケットが秘密性を有するものもあり、また、サーバから発券したチケットのクライアント側による不正利用を如何にして防止するかが

重大な問題である。

【０００４】

【発明が解決しようとする課題】しかしながら、従来の特開平６－２３６４６４号公報に開示された電子チケット発券システム等においては、チケット発券に対する秘密の保持性および不正利用の防止の点において問題がある。

【０００５】そこで、この発明は、送信された電子チケットの不正利用を防止するとともに、チケット発券の秘密の保持性に優れたシステムを提供することを目的とする。

【０００６】

【課題を解決するための手段】上記目的を達成するため、この発明は、電子データを送信するサーバと該サーバから送信された電子データを受信するクライアントと該クライアントで受信した電子データの確認を行う電子データ確認端末とを具備する電子データ送受信システムにおいて、上記サーバは、上記クライアントからの送信要求に対応して暗号化した通し番号を付与した電子データを上記クライアントに送信する電子データ送信手段と、上記電子データ送信手段で送信した電子データを記憶する電子データ記憶手段とを具備し、上記クライアントは、上記電子データ送信手段により上記サーバから送信された電子データを受信することにより上記電子データの受信を行う電子データ受信手段を具備し、上記電子データ確認端末は、上記電子データ受信手段で受信した電子データと上記電子データ記憶手段に記憶した電子データとを照合することにより上記電子データの確認を行う電子データ確認手段を具備することを特徴とする。

【０００７】また、この発明は、電子データを送信するサーバと該サーバから送信された電子データを受信するクライアントと該クライアントで受信した電子データの確認を行う電子データ確認端末とを具備する電子データ送受信システムにおいて、上記クライアントは、上記サーバに対して上記クライアント側で作成した暗号キーワードを含む電子データの送信を要求する送信要求手段を具備し、上記サーバは、上記クライアントからの送信要求に対応して上記暗号キーワードを含む電子データを上記クライアントに送信する電子データ送信手段と、上記電子データ送信手段で送信した電子データを記憶する電子データ記憶手段とを具備し、上記クライアントは、上記電子データ送信手段により上記サーバから送信された電子データを受信する電子データ受信手段を具備し、上記電子データ確認端末は、上記電子データ受信手段で受信した電子データと上記電子データ記憶手段に記憶した電子データとを照合することにより上記電子データの確認を行う電子データ確認手段を具備することを特徴とする。

【０００８】また、この発明は、電子データを送信するサーバと該サーバと回線を介して接続され該サーバから

送信された電子データを受信するクライアントとを具備する電子データ送受信システムにおいて、上記クライアントは、上記電子データの送信要求を生成する送信要求生成手段と、上記送信要求生成手段で発生された送信要求を上記クライアントの秘密鍵を用いて暗号化する第１の暗号化手段と、上記第１の暗号化手段で暗号化された送信要求を上記サーバの公開鍵を用いて暗号化する第２の暗号化手段と、上記第２の暗号化手段で暗号化された送信要求を上記サーバに送信する送信要求手段と、を具備することを特徴とする。

【０００９】また、この発明は、電子データを送信するサーバと該サーバと回線を介して接続され該サーバからから送信された電子データを受信するクライアントとを具備する電子データ送受信システムにおいて、上記クライアントは、上記電子データの送信要求を生成する送信要求生成手段と、上記送信要求生成手段で発生された送信要求に乱数を付与する乱数付与手段と、上記乱数付与手段で乱数が付与された送信要求を上記クライアントの秘密鍵を用いて暗号化する第１の暗号化手段と、上記第１の暗号化手段で暗号化された送信要求を上記サーバの公開鍵を用いて暗号化する第２の暗号化手段と、上記第２の暗号化手段で暗号化された送信要求を上記サーバに送信する送信要求手段と、を具備することを特徴とする。

【００１０】また、この発明は、電子データを送信するサーバと該サーバから送信された電子データを受信するクライアントと該クライアントで受信した電子データの確認を行う電子データ確認端末とを具備する電子データ送受信システムにおいて、上記クライアントは、上記サーバから送信された電子データに対応する上記サーバの秘密鍵を用いて暗号化された電子データを記憶する記憶手段と、上記記憶手段に記憶された上記電子データを取り出す取出手段と、上記取出手段により取出された電子データを上記電子データ確認端末の公開鍵を用いて暗号化する暗号化手段と、上記暗号化手段で暗号化されたデータを上記電子データ確認端末に送信する送信手段と、を具備し、上記電子データ確認端末は、上記送信手段により送信された電子データを受信する受信手段と、上記受信手段で受信した電子データを上記電子データ確認端末の秘密鍵を用いて復号化する復号化手段と、上記復号化手段で復号化した電子データの適否を確認する確認手段と、を具備することを特徴とする

【００１１】

【作用】この発明の電子データ送受信システムにおいて、サーバは、電子データ送信手段により、クライアントからの送信要求に対応して暗号化した通し番号を付与した電子データをクライアントに送信するとともに、電子データ記憶手段により、電子データ送信手段で送信した電子データを記憶する。また、クライアントは、電子データ受信手段により、電子データ送信手段によりサーバから送信された電子データを受信することにより電子データの受信を行う。また、電子データ確認端末は、電子データ確認手段により、電子データ受信手段で受信した電子データと上記電子データ記憶手段に記憶した電子データとを照合することにより電子データの確認を行う。

【００１２】ここで、上記電子データ送信手段は、上記クライアントからの送信要求に対応して電子データを生成する電子データ生成手段と、上記電子データ生成手段で生成された電子データに暗号化した通し番号を付与する通し番号付与手段と、上記通し番号付与手段で暗号化した通し番号が付与された電子データを上記クライアントに送信する送信手段と、を具備して構成することができる。

【００１３】また、上記クライアントは、上記電子データを書き込み可能なカードを有し、上記電子データ送信手段により上記サーバから送信された電子データを受信して上記カードに書き込むことにより上記電子データを受信するように構成することができる。

【００１４】また、上記電子データ確認端末は、上記クライアントで受信した電子データの電子データに付与された暗号化した通し番号を解読することにより上記電子データの確認を行うように構成することができる。

【００１５】また、上記電子データ送信手段は、上記クライアントからの送信要求に対応して電子データを生成する電子データ生成手段と、上記電子データ生成手段で生成された電子データに暗号化した通し番号を付与する通し番号付与手段と、上記通し番号付与手段で暗号化した通し番号が付与された電子データの全体を暗号化する暗号化手段と、上記暗号化手段で暗号化した電子データを上記クライアントに送信する送信手段と、を具備して構成することができる。

【００１６】また、上記クライアントは、上記暗号化手段で暗号化された電子データを解読する解読手段を具備することにより、受信した電子データを確認できるように構成することもできる。

【００１７】また、この発明の電子データ送受信システムにおいて、クライアントは、送信要求手段により、サーバに対してクライアント側で作成した暗号キーワードを含む電子データの送信要求を送信し、サーバは、電子データ送信手段により、クライアントからの送信要求に対応して暗号キーワードを含む電子データをクライアントに送信するとともに、電子データ記憶手段により、電子データ送信手段で送信した電子データを記憶する。また、クライアントは、電子データ受信手段により、電子データ送信手段によりサーバから送信された電子データを受信することにより電子データの受信を行う。また、電子データ確認端末は、電子データ確認手段により、電子データ受信手段で受信した電子データと電子データ記憶手段に記憶した電子データとを照合することにより電

子データの確認を行う。

【００１８】ここで、上記送信要求手段は、上記クライアント側で作成した暗号キーワードを含む電子データの送信要求の全体を暗号化して上記サーバに対して送信するように構成することができる。

【００１９】また、上記電子データ送信手段は、上記暗号キーワードを含む電子データの全体を暗号化して上記サーバに対して送信するように構成することができる。

【００２０】また、上記クライアントは、上記暗号化手段で暗号化された電子データを解読する解読手段を具備することにより、受信した電子データを確認できるように構成することもできる。

【００２１】また、この発明の電子データ送受信システムにおいて、クライアントは、送信要求生成手段により、電子データの送信要求を生成し、第１の暗号化手段により、送信要求生成手段で発生された送信要求をクライアントの秘密鍵を用いて暗号化し、第２の暗号化手段により、第１の暗号化手段で暗号化された送信要求をサーバの公開鍵を用いて更に暗号化し、送信要求手段により、第２の暗号化手段で暗号化された送信要求をサーバに送信する。

【００２２】ここで、上記サーバは、上記送信要求手段により送信された送信要求を受信する送信要求受信手段と、上記送信要求受信手段で受信した送信要求を上記サーバの秘密鍵を用いて復号化する第１の復号化手段と、上記第１の復号化手段で復号化された送信要求を上記クライアントの公開鍵を用いて復号化することにより上記送信要求の適否の照合を行う第１の照合手段と、上記第１の照合手段により上記送信要求が適正であると判定された場合は、上記送信要求に対応する電子データを生成する電子データ生成手段と、上記電子データ生成手段で生成された電子データに暗号化した通し番号を付与する通し番号付与手段と、上記通し番号付与手段で暗号化した通し番号が付与された電子データを上記サーバの秘密鍵を用いて暗号化する第３の暗号化手段と、上記第３の暗号化手段で暗号化された電子データを上記クライアントの公開鍵を用いて暗号化する第４の暗号化手段と、上記第４の暗号化手段で暗号化された電子データを上記サーバに送信する電子データ送信手段と、を具備して構成することがでいる。

【００２３】また、上記クライアントは、上記電子データ送信手段から送信された電子データを受信する電子データ受信手段と、上記電子データ受信手段で受信した電子データを上記クライアントの秘密鍵を用いて復号化する第２の復号化手段と、上記第２の復号化手段で復号化された電子データを上記サーバの公開鍵をを用いて復号化することにより上記電子データの適否の照合を行う第２の照合手段と、上記第２の照合手段で上記電子データが適正であると判定された場合は、上記電子データを記録する記録手段と、を具備して構成することができる。

【００２４】また、この発明の電子データ送受信システムにおいて、クライアントは、送信要求生成手段により、電子データの送信要求を生成し、乱数付与手段により、送信要求生成手段で発生された送信要求に乱数を付与し、第１の暗号化手段により、乱数付与手段で乱数が付与された送信要求をクライアントの秘密鍵を用いて暗号化し、第２の暗号化手段により、第１の暗号化手段で暗号化された送信要求をサーバの公開鍵を用いて更に暗号化し、送信要求手段により、第２の暗号化手段で暗号化された送信要求をサーバに送信する。

【００２５】ここで、上記サーバは、上記送信要求手段により送信された送信要求を受信する送信要求受信手段と、上記送信要求受信手段で受信した送信要求を上記サーバの秘密鍵を用いて復号化する第１の復号化手段と、上記第１の復号化手段で復号化された送信要求を上記クライアントの公開鍵を用いて復号化することにより上記送信要求の適否の照合を行う第１の照合手段と、上記第１の照合手段により上記送信要求が適正であると判定された場合は、上記送信要求に対応する電子データを生成する電子データ生成手段と、上記電子データ生成手段で生成された電子データを上記サーバの秘密鍵を用いて暗号化する第３の暗号化手段と、上記第３の暗号化手段で暗号化された電子データを上記クライアントの公開鍵を用いて暗号化する第４の暗号化手段と、上記第４の暗号化手段で暗号化された電子データを上記サーバに送信する電子データ送信手段と、を具備して構成することができる。

【００２６】また、上記クライアントは、上記電子データ送信手段から送信された電子データを受信する電子データ受信手段と、上記電子データ受信手段で受信した電子データを上記クライアントの秘密鍵を用いて復号化する第２の復号化手段と、上記第２の復号化手段で復号化された電子データを上記サーバの公開鍵をを用いて復号化することにより上記電子データの適否の照合を行う第２の照合手段と、上記第２の照合手段で上記電子データが適正であると判定された場合は、上記電子データを記録する記録手段と、を具備して構成することができる。

【００２７】また、この発明の電子データ送信システムにおいて、クライアントは、記憶手段により、サーバから送信された電子データに対応するサーバの秘密鍵を用いて暗号化された電子データを記憶し、取出手段により、記憶手段に記憶された電子データを取り出し、暗号化手段により、取出手段により取出された電子データを電子データ確認端末の公開鍵を用いて暗号化し、送信手段により、暗号化手段で暗号化されたデータを電子データ確認端末に送信する。また、電子データ確認端末は、受信手段により、送信手段により送信された電子データを受信し、復号化手段により、受信手段で受信した電子データを電子データ確認端末の秘密鍵を用いて復号化し、確認手段により、復号化手段で復号化した電子デー

タの適否を確認する。

【００２８】

【実施例】以下、この発明に係わる電子データ送受信システムの実施例を添付図面に基づいて詳細に説明する。

【００２９】図１は、この発明に係わる電子データ送受信システムの一実施例の概略構成を示すブロック図である。

【００３０】図１において、この電子データ送受信システムは、電子データを送信する電子データサーバ１０を中心に、電子データサーバ（以下、サーバ端末という）１０から送信された電子データを受信するクライアント側に設けられた小型端末（以下、クライアント端末という）２０およびクライアント側で受信した電子データの利用時に該電子データの確認を行う電子データ確認用端末側に設けられた小型端末（以下チェッカ端末という）３０を具備して構成される。

【００３１】ここで、クライアント端末２０およびチェッカ端末３０は、インタネット電話網４０を介してサーバ端末１０に接続されている。

【００３２】なお、図１においては、クライアント端末２０およびチェッカ端末３０をそれぞれ１台ずつ示したが、実際の構成において、クライアント端末２０は一般の家庭または会社に配設されるもので、このクライアント端末２０は多数配設されており、また、チェッカ端末３０は、この電子データの利用箇所、例えば、ホテル、駅、コンサート会場などにそれぞれ配設されるもので、このチェッカ端末３０も多数配設されている。

【００３３】また、クライアント端末２０は、Ｓ－ＲＡＭやＥＥＰ－ＲＯＭ等の半導体メモリを内蔵したＩＣカード等からなるデータ書き込み／読み出し可能な電子データカード（以下、カードという）５０に対してデータを書き込み／読み出しすることができるカードライタ／リーダを有しており、このカード５０に対してサーバ端末１０から送信された電子データの対応する電子データを書き込むことにより電子データを受信するチケット受信処理を行う。

【００３４】また、チェッカ端末３０は、クライアント端末２０によりチケット受信処理されたカード５０からデータを読み出し／書き込みすることのできるカードリーダ／ライタを有しており、このカード５０から所望の電子データを読み出すことにより、この電子データが適正であるか否かのチェックを行う。

【００３５】サーバ端末１０は、クライアント側からの送信要求によりクライアント端末２０を介して電子データを送信する。ここで、この実施例において、電子データの内容としては、

１）ホテル等の利用チケット

２）電車、飛行機、船等のチケット

３）映画館、コンサート等のチケット

３）競馬、競輪等のチケット

等を想定している。

【００３６】また、クライアント側からの送信要求としては、

１）電話回線を用いた電話による音声通信で行われる送信要求

２）電話回線を用いたファクシミリによる画像通信で行われる送信要求

３）電話回線を用いたパーソナルコンピュータ、ファミリコンピュータからのデータ通信で行われる送信要求

４）電子データを送信する店頭における口答による送信要求

５）クライアント端末２０からのインタネット電話網４０を用いた送信要求等が考えられる。

【００３７】いずれの送信要求を採用しても、サーバ端末１０は、この送信要求によりクライアント端末２０を介して電子データを送信する。

【００３８】なお、４）の電子データを送信する店頭における口答による送信要求を採用する場合は、クライアント端末２０は、この電子データを送信する店頭に配設されることになる。

【００３９】なお、以下の説明においては、クライアント側では、５）のクライアント端末２０からのインタネット電話網４０を用いた送信要求を行うものとして各部の動作説明を行う。

【００４０】サーバ端末１０は、クライアント側のクライアント端末２０からの送信要求（チケットの発注）をインタネット電話網４０を介して受信すると、この送信要求に対応する所定の電子データを送信する電子データ送信処理を実行する。ここで、この電子データ送信処理は、サーバ端末１０からインタネット電話網４０を介してクライアント側のクライアント端末２０に送信要求に対応する電子データを送信するとともに、この送信した電子データをサーバ端末１０側に格納することにより行われる。ここで、サーバ端末１０からクライアント端末２０に送信される電子データには、後に詳述するように、クライアント側を特定するための電子署名が付される。

【００４１】また、クライアント側のクライアント端末２０は、このサーバ端末１０からの電子データを受信して、この受信した電子データをカード５０に書き込むことにより電子データの受信処理を行う。

【００４２】また、クライアント側のクライアント端末２０は、このサーバ端末１０からの電子データの受信処理を行った後、この電子データの代金を電子決済により支払うことができる。

【００４３】ところで、この実施例においては、サーバ端末１０による電子データ送信処理において、クライアント側で受信した電子データのクライアント側での不正利用を防止するために、サーバ端末１０からクライアント側のクライアント端末２０に送信する電子データに、

１）暗号化された通し番号を付与する

２）発呼要求の際にクライアント側から送信された暗号キーワードを付与する処理を行い、この電子データを使用する際には、チェッカ端末３０で暗号化された通し番号または暗号キーワードのチェックを行うように構成される。

【００４４】ここで、１）の処理を採用した場合は、通し番号が暗号化されているため、この通し番号をクライアント側では解読することができないため、この通し番号の改竄により同一の電子データを繰り返し何回も使用するという不正利用を防止することができ、また、２）の処理を採用した場合は、この電子データの使用時に暗号キーワードが必要となるため、この電子データの第三者による不正利用を防止することができる。

【００４５】また、この実施例においては、サーバ端末１０からクライアント側のクライアント端末２０へ電子データを送信するに際して、この送信データ全てを暗号化してクライアント端末２０へ送信するように構成される。

【００４６】このような構成によると、サーバ端末１０からクライアント端末２０への電子データの送信途中において、この電子データを第三者に盗聴されたとしても、この第三者によってはこの電子データを解読することはできないので、電子データ送信の秘密性が保持される。この構成は、インタネット電話網４０として、不特定多数がアクセス可能な網を用いる場合等に特に有効である。

【００４７】なお、サーバ端末１０からクライアント端末２０へ送信される電子データを暗号化する構成において、クライアント側でこの暗号化した電子データを解読することができるように構成すれば、クライアント側で受信した電子データの内容の確認を行うことができる。なお、クライアント側で暗号化した電子データを解読することができるように構成した場合で、電子データに暗号化された通し番号を付与する構成をとった場合も、この暗号化された通し番号はクライアント側では解読することができないようにすれば、クライアント側により通し番号を改竄して同一の電子データを繰り返し何回も使用するという不正重複利用を防止することができる。

【００４８】また、チェッカ端末３０は、この電子データの利用箇所において、利用電子データが適正であるか否かのチェックを行う。具体的には、クライアント側での電子データの受信は、上述したように、サーバ端末１０から送信された電子データをカード５０に書き込むことにより行われるので、この受信した電子データを利用する場合は、この電子データが書き込まれたカード５０をこの電子データの利用箇所まで利用者が携帯して行き、このカード５０をこの電子データの利用箇所に配設されたチェッカ端末３０に挿入することにより、この電子データのチェックが行われる。

【００４９】このチェックにおいて、この電子データが適正なものであるとすると、この電子データの利用が可能になる。例えば、この電子データがホテル等の利用チケットの場合は、このホテルの利用が可能になり、電車、飛行機、船等のチケットの場合は、電車、飛行機、船等の利用が可能になり、映画館、コンサート等のチケットの場合は映画館、コンサート等の入場が可能になり、競馬、競輪等のチケットの場合は、馬券、車券等の購入が可能になる。

【００５０】このチェッカ端末３０には、サーバ端末１０から後に詳述する公開鍵および送信したチェックデータが配布されており、チェッカ端末３０では、この公開鍵を用いてカード５０に書き込まれた電子データを解読し、その結果この電子データが適正であるか否かのチェックを行う。

【００５１】図２は、サーバ端末１０の具体的構成をブロック図で示したものである。図２において、このサーバ端末１０は、基本ブロック１００と送信した電子データ等を格納するデータベース１２を具備して構成される。

【００５２】ここで、基本ブロック１００は、図３に示しように、識別子発生装置１０１、時計１０２、電源１０３、通信部１０４、作業域１０５、暗号処理装置１１０を具備して構成され、暗号処理装置１１０は、電子署名装置１１１、電子署名参照装置１１２、暗号化装置１１３、復号化装置１１４、鍵管理装置１２０を具備し、鍵管理装置１２０は、公開鍵管理装置１２１、秘密鍵管理装置１２２を具備している。

【００５３】ここで、識別子発生装置１０１はこの基本ブロック１００が搭載された機器の識別子を発生するもの、時計１０２は時刻を計時するもので、電子データの送信時刻等を管理するもの、電源１０３はこの基本ブロック１００が搭載された機器の駆動電源を与えるもので、商用電源からの供給を受けるものまたは電池から構成されるもの、通信部１０４はこの基本ブロック１００が搭載された機器と他の機器との間の通信を行うもの、作業域１０５は、この基本ブロック１００が搭載された機器の各種データ処理を行う箇所、暗号処理装置１１０はこの基本ブロック１００が搭載された機器における各種暗号処理を行うものである。

【００５４】また、電子署名装置１１１は後に詳述する電子署名処理を行うもの、電子署名参照装置１１２は後に詳述する電子署名参照処理を行うもの、暗号化装置１１３はデータの暗号化処理を行うもの、復号化装置１１４は暗号化されたデータの復号化処理を行うもの、鍵管理装置１２０は、電子署名装置１１１による電子署名処理、電子署名参照装置１１２による電子署名参照処理、暗号化装置１１３による暗号化処理、復号化装置１１４による復号化処理で用いる公開鍵および秘密鍵を管理するものである。

15

【００５５】また、公開鍵管理装置１２１は上記公開鍵を管理するもの、秘密鍵管理装置１２２は上記秘密鍵を管理するものである。なお、このこの公開鍵および秘密鍵については後に詳述する。

【００５６】図４は、クライアント端末２０の具体的構成をブロック図で示したものである。図４において、このクライアント端末２０は、基本ブロック１００、入力装置２１、記憶域２２、表示装置２３、記録装置２４、電子決済装置２５を具備して構成される。

【００５７】ここで、基本ブロック１００は図３に詳述したものと同一のものである。

【００５８】また、入力装置２１はこのクライアント端末２０を動作させるための各種データおよびコマンドを入力するもの、記憶域２２はこのクライアント端末２０の処理のための作業域を構成するもの、表示装置２３はこのクライアント端末２０の動作状態等を含む各種情報を表示するもの、記録装置２４は、例えばサーバ端末１０から受信した電子データ等を記録するもの、電子決済装置２５は電子データを受信した際の代金を電子決済するものである。

【００５９】図５は、チェッカ端末３０の具体的構成をブロック図で示したものである。図５において、このチェッカ端末３０は、基本ブロック１００、確認装置３１、表示装置３２を具備して構成される。

【００６０】ここで、基本ブロック１００は図３に詳述したものと同一のものである。

【００６１】また、確認装置３１は利用電子データが適正か否かを確認するもの、表示装置３２は確認装置３１による確認結果等を表示するものである。

【００６２】図６は、図１に示した電子データ送信システムにおける電子データ予約手順の具体例を示したもので、この図６の示すものにおいては、暗号化した通し番号を用いた場合におけるクライアント側のクライアント端末２０およびサーバ側のサーバ端末１０の動作を示している。

【００６３】ところで、この実施例においてはクライアント側およびサーバ側における電子署名および暗号化／復号化処理のために、クライアント側のクライアント端末２０は、秘密鍵Ｋｃｓおよび公開鍵Ｋｃｐを有しており、また、サーバ側のサーバ端末１０は、秘密鍵Ｋｓｓおよび公開鍵Ｋｓｐを有している。

【００６４】ここで、秘密鍵Ｋｃｓは、クライアント側における電子署名に用いるもので、この秘密鍵Ｋｃｓで暗号化されたデータは、対応する公開鍵Ｋｃｐを用いることにより、サーバ側で復号化することができる。

【００６５】また、公開鍵Ｋｓｐは、クライアント側における暗号化に用いるもので、公開鍵Ｋｓｐで暗号化されたデータは、対応する秘密鍵Ｋｓｓを用いないと復号化できない。

【００６６】また、秘密鍵Ｋｓｓはサーバ側における電子署名に用いるもので、この秘密鍵Ｋｓｓで暗号化されたデータは、対応する公開鍵Ｋｓｐを用いることにより、クライアント側で復号化することができる。

16

【００６７】また、公開鍵Ｋｃｐは、サーバ側における暗号化に用いるもので、公開鍵Ｋｃｐで暗号化されたデータは、対応する秘密鍵Ｋｃｓを用いないと復号化できない。

【００６８】図６において、クライアント側からサーバ側に対して送信要求をする場合は、まず、この送信要求に対応するリクエストＲを生成する（ステップ２０１）。そして、このリクエストＲをクライアントの秘密鍵Ｋｃｓで暗号化することにより電子署名を行う（ステップ２０２）。

【００６９】次に、この電子署名を行ったリクエストＲ（Ｋｃｓ）を更にサーバの公開鍵Ｋｓｐで暗号化し（ステップ２０３）、この暗号化したリクエストＲ（Ｋｃｓ、Ｋｓｐ）をサーバ側に送信する（ステップ２０４）。

【００７０】サーバ側では、このリクエストＲ（Ｋｃｓ、Ｋｓｐ）を受信し（ステップ２０５）、この受信したリクエストＲ（Ｋｃｓ、Ｋｓｐ）をサーバの秘密鍵Ｋｓｓで復号化する（ステップ２０６）。

【００７１】そして、この復号化したリクエストＲ（Ｋｃｓ）をクライアントの公開鍵Ｋｃｐで復号化することにより送信要求に係わるクライアント側の電子署名の照合を行う（ステップ２０７）。

【００７２】このステップ２０７の電子署名照合の結果、この電子署名が適正でないと判断した場合は（ステップ２０７でＮＯ）、この送信要求を無視する（ステップ２０８）。

【００７３】また、このステップ２０７の電子署名照合の結果、この電子署名が適正であると判断した場合は（ステップ２０７でＯＫ）、次に、この送信要求が予約処理かを調べる（ステップ２０９）。ここで、予約処理でないと判断した場合は（ステップ２０９でＮＯ）、送信要求の拒否通知Ｔを生成し（ステップ２１２）、ステップ２１３に移行する。

【００７４】また、ステップ２０９において、この送信要求が予約処理であると判断した場合は（ステップ２０９でＯＫ）、この送信要求に対応する電子データＴ´（＝Ｒ（Ｋｃｓ）＋α）を生成し（ステップ２１０）、次に、この電子データＴ´に暗号化した通し番号を付与して（ステップ２１１）、電子データＴ（＝Ｔ´＋通し番号）を生成し、ステップ２１３に移行する。

【００７５】ステップ２１３では、電子データまたは拒否通知Ｔをサーバの秘密鍵Ｋｓｓで暗号化することにより電子署名を行い、この電子署名した情報Ｔ（Ｋｓｓ）を更にクライアントの公開鍵Ｋｃｐで暗号化し（ステップ２１４）、この暗号化した情報Ｔ（Ｋｓｓ、Ｋｃｐ）をクライアント側に送信する（ステップ２１５）。

【００７６】クライアント側では、この情報Ｔ（Ｋｓｓ、Ｋｃｐ）を受信し（ステップ２１６）、この受信した情報Ｔ（Ｋｓｓ、Ｋｃｐ）をクライアントの秘密鍵Ｋｃｓで復号化する（ステップ２１７）。

【００７７】そして、この復号化した情報Ｔ（Ｋｓｓ）をサーバの公開鍵Ｋｓｐで復号化することによりサーバ側の電子署名の照合を行う（ステップ２１８）。

【００７８】このステップ２１８の電子署名照合の結果、この電子署名が適正でないと判断した場合は（ステップ２１８でＮＯ）、この情報を無視する（ステップ２１９）。

【００７９】また、このステップ２１８の電子署名照合の結果、この電子署名が適正であると判断した場合は（ステップ２１８でＯＫ）、次に、この情報Ｔから送信要求の結果確認を行う（ステップ２２０）。

【００８０】この結果確認により、情報Ｔが拒否通知である場合は（ステップ２２０でＮＯ）、所定の予約エラー処理を実行する（ステップ２２１）。

【００８１】また、この結果確認により、情報Ｔが送信要求に対応する電子データである場合は（ステップ２２０でＯＫ）、記録装置に記録する（ステップ２２２）とともに、電子データＴ（Ｋｓｓ）の格納を行う（ステップ２２３）。

【００８２】なお、ステップ２１８～２２２の処理を行うことなく、ステップ２１７から直接ステップ２２３に移行するように構成してもよい。

【００８３】図７は、図１に示した電子データ送信システムにおける電子データ予約手順の他の具体例を示したもので、この図７の示すものにおいては、乱数を用いた場合におけるクライアント側のクライアント端末２０およびサーバ側のサーバ端末１０の動作を示している。

【００８４】図７において、クライアント側からサーバ側に対して送信要求をする場合は、まず、この送信要求に対応するリクエストＲ´を生成する（ステップ３０１）。

【００８５】そして、このリクエストＲ´に乱数を付与する（ステップ３０２）。その後、この乱数が付与されたリクエストＲ（Ｒ´＋乱数）をクライアントの秘密鍵Ｋｃｓで暗号化することにより電子署名を行う（ステップ３０３）。

【００８６】次に、この電子署名を行ったリクエストＲ（Ｋｃｓ）を更にサーバの公開鍵Ｋｓｐで暗号化し（ステップ３０４）、この暗号化したリクエストＲ（Ｋｃｓ、Ｋｓｐ）をサーバ側に送信する（ステップ３０５）。

【００８７】サーバ側では、このリクエストＲ（Ｋｃｓ、Ｋｓｐ）を受信し（ステップ３０６）、この受信したリクエストＲ（Ｋｃｓ、Ｋｓｐ）をサーバの秘密鍵Ｋｓｓで復号化する（ステップ３０７）。

【００８８】そして、この復号化したリクエストＲ（Ｋｃｓ）をクライアントの公開鍵Ｋｃｐで復号化することにより送信要求に係わるクライアント側の電子署名の照合を行う（ステップ３０８）。

【００８９】このステップ３０８の電子署名照合の結果、この電子署名が適正でないと判断した場合は（ステップ３０８でＮＯ）、この送信要求を無視する（ステップ３０９）。

【００９０】また、このステップ３０８の電子署名照合の結果、この電子署名が適正であると判断した場合は（ステップ３０８でＯＫ）、次に、この送信要求が予約処理かを調べる（ステップ３１０）。ここで、予約処理でないと判断した場合は（ステップ３１０でＮＯ）、送信要求の拒否通知Ｔを生成し（ステップ３１２）、ステップ３１３に移行する。

【００９１】また、ステップ３１０において、この送信要求が予約処理であると判断した場合は（ステップ３１０でＯＫ）、この送信要求に対応する電子データＴ（＝Ｒ（Ｋｃｓ）＋α）を生成し（ステップ３１１）、ステップ３１３に移行する。

【００９２】ステップ３１３では、電子データまたは拒否通知Ｔをサーバの秘密鍵Ｋｓｓで暗号化することにより電子署名を行い、この電子署名した情報Ｔ（Ｋｓｓ）を更にクライアントの公開鍵Ｋｃｐで暗号化し（ステップ３１４）、この暗号化した情報Ｔ（Ｋｓｓ、Ｋｃｐ）をクライアント側に送信する（ステップ３１５）。

【００９３】クライアント側では、この情報Ｔ（Ｋｓｓ、Ｋｃｐ）を受信し（ステップ３１６）、この受信した情報Ｔ（Ｋｓｓ、Ｋｃｐ）をクライアントの秘密鍵Ｋｃｓで復号化する（ステップ３１７）。

【００９４】そして、この復号化した情報Ｔ（Ｋｓｓ）をサーバの公開鍵Ｋｓｐで復号化することによりサーバ側の電子署名の照合を行う（ステップ３１８）。

【００９５】このステップ３１８の電子署名照合の結果、この電子署名が適正でないと判断した場合は（ステップ３１８でＮＯ）、この情報を無視する（ステップ３１９）。

【００９６】また、このステップ３１８の電子署名照合の結果、この電子署名が適正であると判断した場合は（ステップ３１８でＯＫ）、次に、この情報Ｔから送信要求の結果確認を行う（ステップ３２０）。

【００９７】この結果確認により、情報Ｔが拒否通知である場合は（ステップ３２０でＮＯ）、所定の予約エラー処理を実行する（ステップ３２１）。

【００９８】また、この結果確認により、情報Ｔが送信要求に対応する電子データである場合は（ステップ３２０でＯＫ）、記録装置に記録する（ステップ３２２）とともに、電子データＴ（Ｋｓｓ）の格納を行う（ステップ３２３）。

【００９９】なお、ステップ３１８～３２２の処理を行うことなく、ステップ３１７から直接ステップ３２３に

移行するように構成してもよい。

【０１００】図８は、図１に示した電子データ送信システムにおける電子データ利用手順の具体例を示したもので、図８においてはクライアント側のクライアント端末２０および電子データ確認用端末側のチェック端末３０の動作を示している。

【０１０１】なお、この実施例においてはクライアント側および電子データ確認用端末側における電子署名および暗号化／復号化処理のために、クライアント側のクライアント端末２０は、秘密鍵Ｋｃｓおよび公開鍵Ｋｃｐを有しており、また、電子データ確認用端末側のチェック端末３０は、秘密鍵Ｋｔｓおよび公開鍵Ｋｔｐを有している。

【０１０２】図８において、クライアント側ではサーバ側で電子署名された電子データＴ（Ｋｓｓ）が格納されている（ステップ４０１）。まず、クライアント側では、格納されているチケット、すなわち、電子データＴ（Ｋｓｓ）を取り出し（ステップ４０２）、この電子データＴ（Ｋｓｓ）を確認用端末の公開鍵Ｋｔｐで暗号化し（ステップ３０４）、この暗号化した電子データＴ（Ｋｓｓ、Ｋｔｐ）を電子データ確認用端末側に送信する（ステップ４０４）。

【０１０３】電子データ確認用端末側では、この電子データＴ（Ｋｓｓ、Ｋｔｐ）を受信し（ステップ４０５）、この受信した電子データＴ（Ｋｓｓ、Ｋｔｐ）を確認用端末の秘密鍵Ｋｔｓで復号化する（ステップ４０６）。

【０１０４】そして、この復号化した電子データＴ（Ｋｓｓ）をサーバの公開鍵Ｋｓｐで復号化することにより電子署名の照合を行う（ステップ４０７）。

【０１０５】このステップ４０７の電子署名照合の結果、この電子署名が適正でないと判断した場合は（ステップ４０７でＮＯ）、この電子データＴ（Ｋｓｓ）を無視する（ステップ４０８）。

【０１０６】また、このステップ４０７の電子署名照合の結果、この電子署名が適正であると判断した場合は（ステップ４０７でＯＫ）、次に、電子データＴ（Ｋｓｓ）の内容確認を行う（ステップ４０９）。

【０１０７】この内容確認の結果、電子データＴ（Ｋｓｓ）が適正でない場合は（ステップ４０９でＮＯ）、所定のエラー処理を行う（ステップ４１０）。

【０１０８】また、この内容確認の結果、電子データＴ（Ｋｓｓ）が適正ある場合は（ステップ４０９でＯＫ）、次に、電子データＴ（Ｋｓｓ）に付与されている暗号化された通し番号に重複があるか否かの番号重複確認を行う（ステップ４１１）。

【０１０９】ここで、通し番号に重複ありと判断された場合は、エラーとして所定のエラー処理を行う（ステップ４１２）。

【０１１０】また、ステップ４１１で通し番号に重複なしと判断された場合は、電子データＴ（Ｋｓｓ）に対応する所定のチケット内容実行を行う（ステップ４１３）。

【０１１１】

【発明の効果】以上説明したように、この発明の電子データ送受信システムによれば、サーバは、電子データ送信手段により、クライアントからの送信要求に対応して暗号化した通し番号を付与した電子データをクライアントに送信するとともに、電子データ記憶手段により、電子データ送信手段で送信した電子データを記憶し、また、クライアントは、電子データ受信手段により、電子データ送信手段によりサーバから送信された電子データを受信することにより電子データの受信を行い、また、電子データ確認端末は、電子データ確認手段により、電子データ受信手段で受信した電子データと上記電子データ記憶手段に記憶した電子データとを照合することにより電子データの確認を行うように構成したので、送信された電子データの不正利用を防止するとともに、チケット送信の秘密の保持性に優れた電子データ送受信システムを提供することができるという効果を奏する。

【図面の簡単な説明】

【図１】この発明に係わる電子データ送受信システムの一実施例の概略構成を示すブロック図。

【図２】図１に示したサーバ端末の具体的構成を示すブロック図。

【図３】図２に示した基本ブロックの詳細構成を示すブロック図。

【図４】図１に示したクライアント端末の具体的構成を示すブロック図。

【図５】図１に示したチェッカ端末の具体的構成を示すブロック図。

【図６】図１に示した電子データ送信システムにおける電子データ予約手順の具体例を示したフローチャート。

【図７】図１に示した電子データ送信システムにおける電子データ予約手順の他の具体例を示したフローチャート。

【図８】図１に示した電子データ送信システムにおける電子データ利用手順の具体例を示したフローチャート。

【符号の説明】

１０　電子データサーバ（サーバ端末）
１２　データベース
２０　小型端末（クライアント端末）
２１　入力装置
２２　記憶域
２３　表示装置
２４　記録装置
２５　電子決済装置
３０　小型端末（チェッカ端末）
３１　確認装置
３２　表示装置

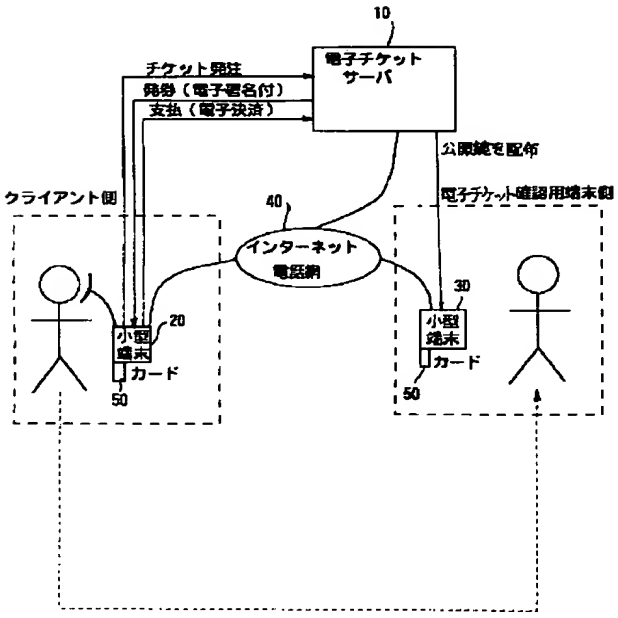
21

４０　インタネット電話網
５０　電子チケットカード（カード）
１００　基本ブロック
１０１　識別子発生装置
１０２　時計
１０３　電源
１０４　通信部
１０５　作業域

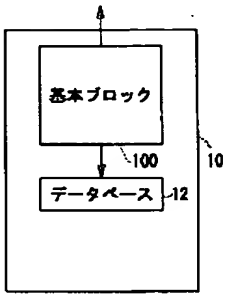
22

１１０　暗号処理装置
１１１　電子署名装置
１１２　電子署名照合装置
１１３　暗号化装置
１１４　復号化装置
１２０　鍵管理装置
１２１　公開鍵管理装置
１２２　秘密鍵管理装置

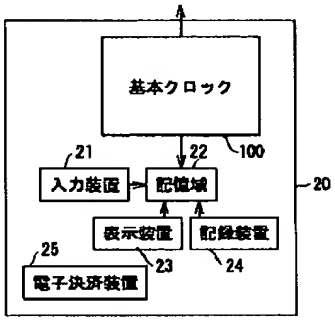
【図１】



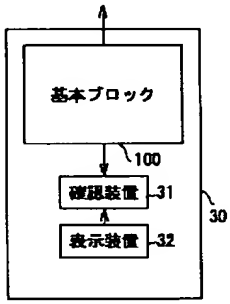
【図２】



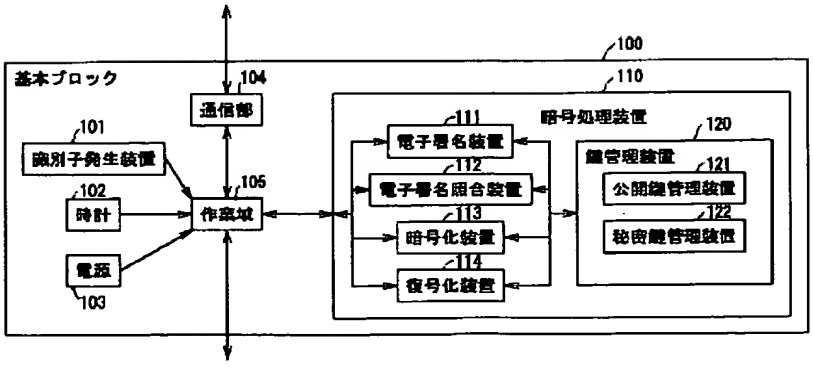
【図４】



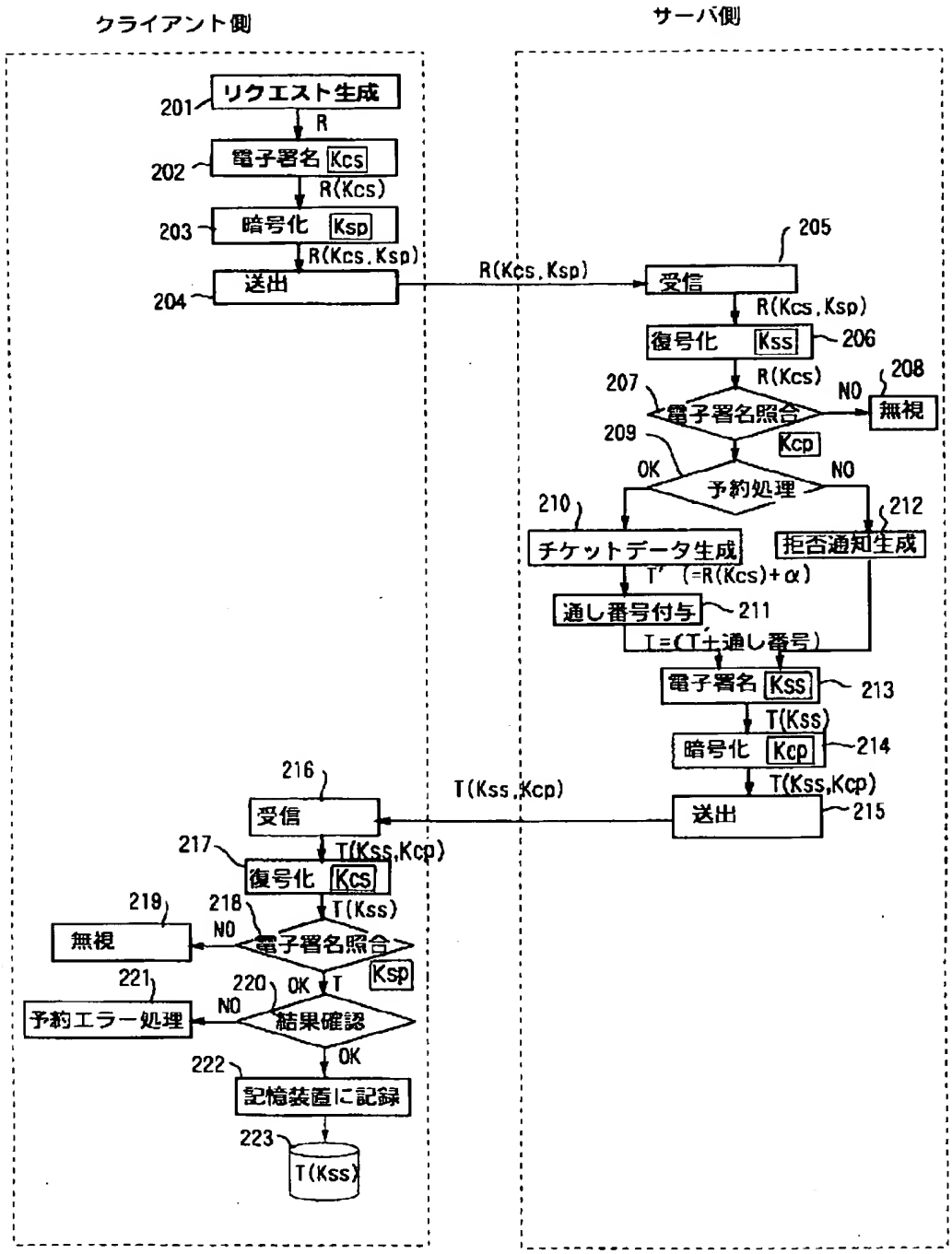
【図５】



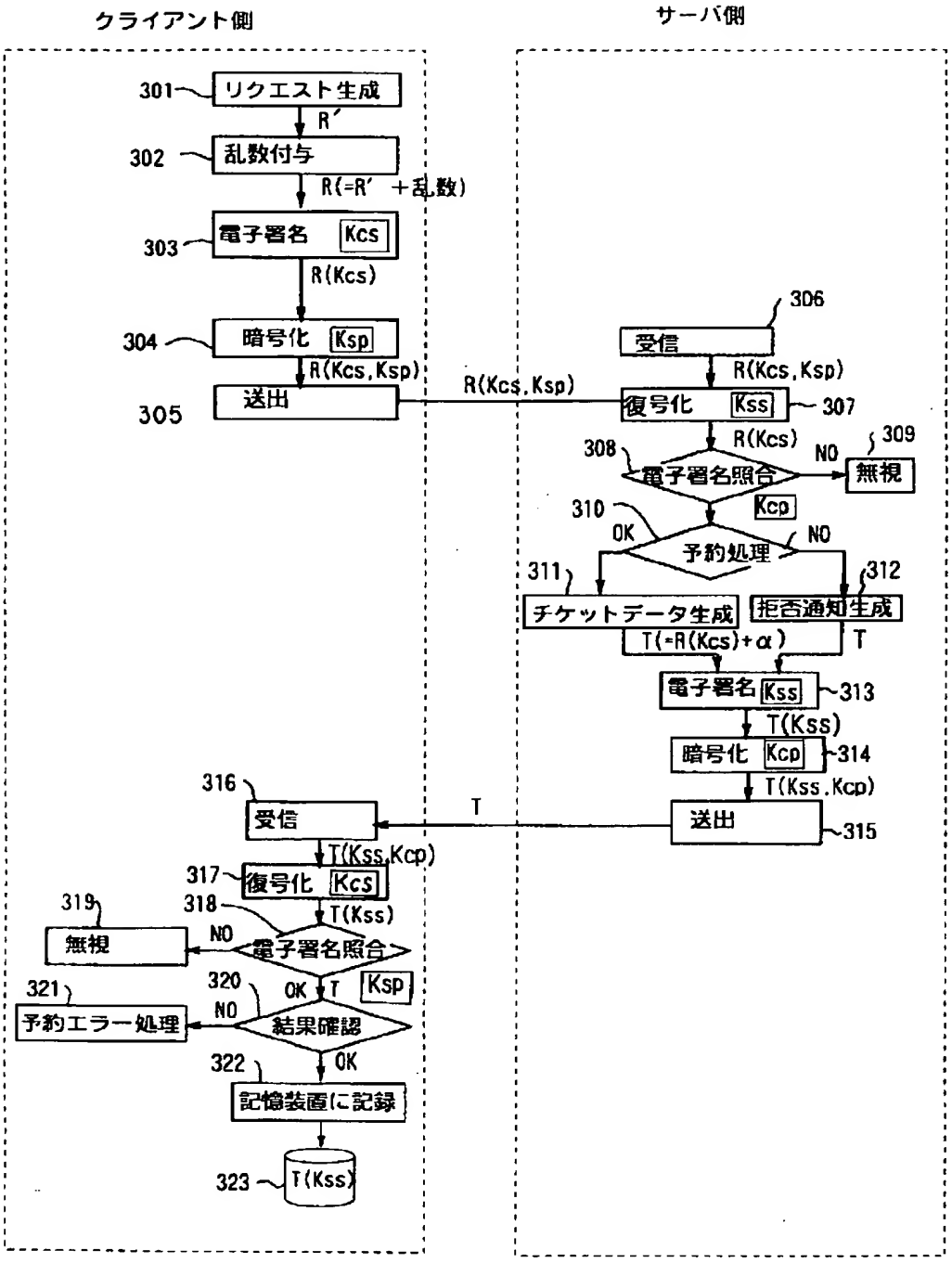
【図３】



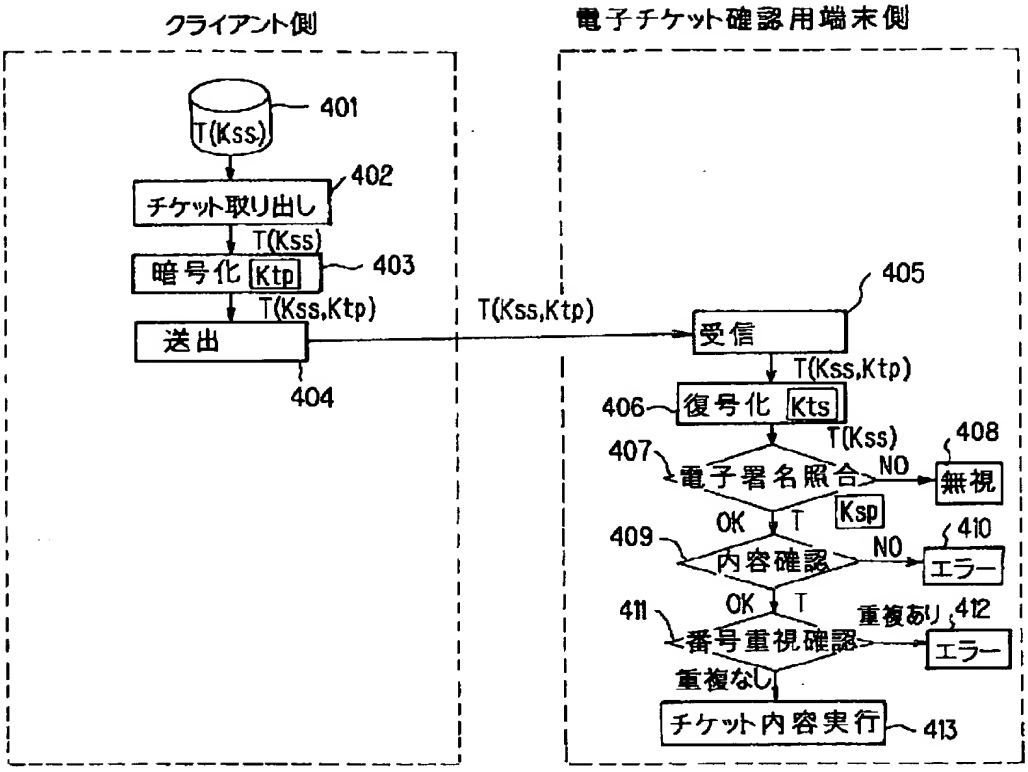
【図６】


クライアント側
サーバ側
リクエスト生成
201
R
電子署名 Kcs
202
R(Kcs)
暗号化 Ksp
203
R(Kcs,Ksp)
送出
204
R(Kcs,Ksp)
205
受信
R(Kcs,Ksp)
復号化 Kss
206
R(Kcs)
207
電子署名照合
NO
208
無視
Kcp
209
OK
予約処理
NO
210
チケットデータ生成
212
拒否通知生成
T' (=R(Kcs)+α)
通し番号付与
211
T=(T'+通し番号)
電子署名 Kss
213
T(Kss)
暗号化 Kcp
214
T(Kss,Kcp)
送出
215
T(Kss,Kcp)
216
受信
T(Kss,Kcp)
217
復号化 Kcs
T(Kss)
218
219
無視
NO
電子署名照合
Ksp
221
220
OK
T
予約エラー処理
NO
結果確認
OK
222
記憶装置に記録
223
T(Kss)

【図７】


クライアント側
サーバ側
301
リクエスト生成
R′
302
乱数付与
R(=R′ ＋乱数)
303
電子署名 Kcs
R(Kcs)
304
暗号化 Ksp
R(Kcs,Ksp)
305
送出
R(Kcs,Ksp)
306
受信
R(Kcs,Ksp)
復号化 Kss
307
R(Kcs)
308
電子署名照合
NO
309
無視
Kcp
310
OK
予約処理
NO
311
チケットデータ生成
312
拒否通知生成
T(=R(Kcs)+α)
T
電子署名 Kss
313
T(Kss)
暗号化 Kcp
314
T(Kss,Kcp)
送出
315
T
316
受信
T(Kss,Kcp)
317
復号化 Kcs
T(Kss)
318
319
無視
NO
電子署名照合
Kcp
320
OK
T
321
予約エラー処理
NO
結果確認
OK
322
記憶装置に記録
323
T(Kss)

【図８】


クライアント側
電子チケット確認用端末側
401
T(Kss)
402
チケット取り出し
T(Kss)
暗号化 Ktp
403
T(Kss,Ktp)
送出
404
T(Kss,Ktp)
405
受信
T(Kss,Ktp)
406
復号化 Kts
T(Kss)
407
電子署名照合
NO
408
無視
OK
T
Ksp
409
内容確認
NO
410
エラー
OK
T
411
番号重視確認
重複あり
412
エラー
重複なし
チケット内容実行
413